

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of

Shinya SHIMASAKI

Conf.

Application No. NEW NON-PROVISIONAL

Group

Filed March 25, 2004

Examiner

PSEUDO-RANDOM NUMBER GENERATOR

CLAIM TO PRIORITY

Assistant Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

March 25, 2004

Sir:

Applicant(s) herewith claim(s) the benefit of the priority filing date of the following application(s) for the above-entitled U.S. application under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55:

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
JAPAN	2003-095596	March 31, 2003

Certified copy(ies) of the above-noted application(s) is(are) attached hereto.

Respectfully submitted,

YOUNG & THOMPSON



---

Benoit Castel, Reg. No. 35,041  
745 South 23<sup>rd</sup> Street  
Arlington, VA 22202  
Telephone (703) 521-2297  
Telefax (703) 685-0573  
703) 979-4709

BC/ma

Attachment(s): 1 Certified Copy(ies)

日本国特許庁  
JAPAN PATENT OFFICE

US  
03/266  
g

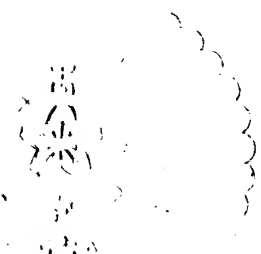
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月31日  
Date of Application:

出願番号 特願2003-095596  
Application Number:  
[ST. 10/C]: [J.P.2003-095596]

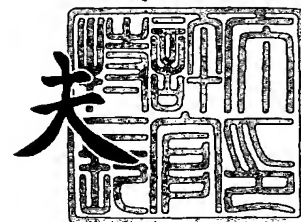
出願人 NECマイクロシステム株式会社  
Applicant(s):



2004年 2月26日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2004-3013791

【書類名】 特許願

【整理番号】 01220093

【提出日】 平成15年 3月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 7/58

【発明者】

【住所又は居所】 神奈川県川崎市中原区小杉町 1 丁目 4 0 3 番 5 3 エヌ  
イーシーマイクロシステム株式会社内

【氏名】 嶋崎 真也

【特許出願人】

【識別番号】 000232036

【氏名又は名称】 エヌイーシーマイクロシステム株式会社

【代理人】

【識別番号】 100088328

【弁理士】

【氏名又は名称】 金田 暢之

【電話番号】 03-3585-1882

【選任した代理人】

【識別番号】 100106297

【弁理士】

【氏名又は名称】 伊藤 克博

【選任した代理人】

【識別番号】 100106138

【弁理士】

【氏名又は名称】 石橋 政幸

【手数料の表示】

【予納台帳番号】 089681

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9712889

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 擬似乱数発生回路

【特許請求の範囲】

【請求項 1】 直列に接続された複数のレジスタ、前記レジスタの所定出力の排他的論理和を出力する第 1 の排他的論理和回路、及び外部から供給される入力データと前記第 1 の排他的論理和回路の出力信号との排他的論理和を前記複数のレジスタのうちの先頭のレジスタに入力する第 2 の排他的論理和回路を備えたりニアフィードバックレジスタと、

一定周期の第 1 のクロック、及び前記第 1 のクロックに同期させた前記第 1 のクロックと異なる周波数の第 2 のクロックを用いて、前記リニアフィードバックレジスタを動作させるためのクロックであるシフトクロック及び前記入力データを生成する信号生成回路と、  
を有する擬似乱数発生回路。

【請求項 2】 一定周期の第 3 のクロックを生成する発振回路と、

前記第 3 のクロックと前記第 3 のクロックに対して非同期な第 4 のクロックとの排他的論理和を前記シフトクロックとして前記リニアフィードバックレジスタに供給し、前記第 4 のクロックを前記入力データとして前記リニアフィードバックレジスタに供給するPre-SEED生成回路と、  
を有し、

前記リニアフィードバックレジスタは、

電源投入時に、前記発振回路が安定発振する前の不安定な前記第 3 のクロックを前記シフトクロックとして用いることで初期値の元になるPre-SEEDを生成する請求項 1 記載の擬似乱数発生回路。

【請求項 3】 前記信号生成回路は、

前記第 1 のクロック、及び前記第 1 のクロックを分周したクロックを所定の周期で切り換えた前記シフトクロックを出力する請求項 1 または 2 記載の擬似乱数発生回路。

【請求項 4】 前記リニアフィードバックレジスタで生成された乱数を所定の周期毎に読み出すためのアクセスコントローラを有する請求項 1 乃至 3 のいづ

れか 1 項記載の擬似乱数発生回路。

【請求項 5】 前記リニアフィードバックレジスタの出力データと前記リニアフィードバックレジスタが備える複数のレジスタに書き込むための任意のデータである書き込み信号との排他的論理和を出力する書き込み回路を有し、

前記リニアフィードバックレジスタは、

前記レジスタの値を前記書き込み回路の出力データで書き換えるための書換え手段を有する請求項 1 乃至 4 のいずれか 1 項記載の擬似乱数発生回路。

【請求項 6】 前記リニアフィードバックレジスタが備える複数のレジスタの数は、前記乱数のビット数よりも多い請求項 1 乃至 5 のいずれか 1 項記載の擬似乱数発生回路。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、リニアフィードバックシフトレジスタ (Linear Feedback Shift Register、以下、LFSR と略す) を用いて擬似乱数を生成する擬似乱数発生回路に関する。

##### 【0002】

##### 【従来の技術】

従来より、暗号アルゴリズム等に乱数が用いられているが、この乱数としては扱いやすさや処理の簡単さから真性乱数よりもソフトウェアでも容易に生成可能な擬似乱数を用いることが多い。

##### 【0003】

擬似乱数を発生する擬似乱数発生回路としては LFSR を用いて長周期の乱数列を生成する構成が一般的である。LFSR は直列に接続された複数のレジスタの所定出力を排他的論理和回路 (以下、XOR 回路と称す) を介して先頭のレジスタにフィードバックさせる構成であり、フィードバック部に XOR 回路を設けることで比較的長周期の乱数列を得ることが可能になる。

##### 【0004】

例えば、 $n$  個のレジスタで構成される LFSR から得られる乱数列の周期は  $n$

次の線形最大周期列（M系列と呼ばれる） $2^n - 1$ となる。なお、LFSRから得られる乱数列は、上記M系列の乱数を繰り返し発生したものであり、LFSRの周期とは、このM系列の数を示し、時間を表すものではない。

#### 【0005】

擬似乱数を用いて暗号文を生成する暗号回路等では、擬似乱数系列あるいは擬似乱数系列の生成論理が判明すると、入手した暗号文から元の平文を再生することが可能になるため、予測不可能な擬似乱数系列を効率的に生成することが重要になる。

#### 【0006】

擬似乱数系列あるいは擬似乱数系列の生成論理は、乱数のビット数に対してLFSRの次数 $n$ （レジスタの数）を増やすほど、その解読が困難になるが、回路規模等の制約から少ないビット数のLFSRしか使用できない場合がある。そこで、少ないビット数のLFSRで生成する擬似乱数の乱数性を高めるために、周波数の異なる複数のクロックを備え、各レジスタを動作させるためのクロック（シフトクロック）をLFSRの所定出力を用いて切り換える構成が特許文献1に記載されている。

#### 【0007】

##### 【特許文献1】

特許2937919号

#### 【0008】

##### 【発明が解決しようとする課題】

シフトクロックが固定の場合、LFSRは所定の初期値（SEED）から各周期毎に同一の乱数列を繰り返し発生する。それに対して上記従来の擬似乱数発生回路では、LFSRの所定出力を用いてシフトクロックを切り換えることで、シフト動作のタイミングにばらつきが発生するため、見かけ上の周期がLFSRのビット数で決まる周期よりも長くなる。

#### 【0009】

しかしながら、このような構成では、シフトクロックのばらつきによって乱数の発生タイミングは変わるが、生成されるSEEDや乱数の順序はシフトクロック

クの固定時に生成される乱数の順序に等しくなる。すなわち、図 11 に示すように、乱数は一定時間毎に生成されずに、ランダムな時間間隔で生成されるが（但し、短い期間で見ると、一定時間毎に連続して発生（点在）する）、シフトクロックの固定時に生成される乱数の順序を乱すものではない。そのため、シフトクロックの固定時よりも乱数性は高くなるが、擬似乱数系列あるいは擬似乱数系列の生成論理が特定されるおそれは依然として高く、乱数性が十分に高いとは言えない問題があった。

#### 【0010】

本発明は上記したような従来の技術が有する問題点を解決するためになされたものであり、高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を提供することを目的とする。

#### 【0011】

##### 【課題を解決するための手段】

上記目的を達成するため本発明の擬似乱数発生回路は、直列に接続された複数のレジスタ、前記レジスタの所定出力の排他的論理和を出力する第 1 の排他的論理和回路、及び外部から供給される入力データと前記第 1 の排他的論理和回路の出力信号との排他的論理和を前記複数のレジスタのうちの先頭のレジスタに入力する第 2 の排他的論理和回路を備えたりニアフィードバックレジスタと、

一定周期の第 1 のクロック、及び前記第 1 のクロックに同期させた前記第 1 のクロックと異なる周波数の第 2 のクロックを用いて、前記リニアフィードバックレジスタを動作させるためのクロックであるシフトクロック及び前記入力データを生成する信号生成回路と、  
を有する構成である。

#### 【0012】

このとき、一定周期の第 3 のクロックを生成する発振回路と、

前記第 3 のクロックと前記第 3 のクロックに対して非同期な第 4 のクロックとの排他的論理和を前記シフトクロックとして前記リニアフィードバックレジスタに供給し、前記第 4 のクロックを前記入力データとして前記リニアフィードバックレジスタに供給する Pre-SEED 生成回路と、



を有し、

前記リニアフィードバックレジスタは、

電源投入時に、前記発振回路が安定発振する前の不安定な前記第3のクロックを前記シフトクロックとして用いることで初期値の元になるPre-SEEDを生成してもよく、

前記信号生成回路は、

前記第1のクロック、及び前記第1のクロックを分周したクロックを所定の周期で切り換えた前記シフトクロックを出力してもよい。

#### 【0013】

また、前記リニアフィードバックレジスタで生成された乱数を所定の周期毎に読み出すためのアクセスコントローラを有していてもよく、

前記リニアフィードバックレジスタの出力データと前記リニアフィードバックレジスタが備える複数のレジスタに書き込むための任意の乱数データである書き込み信号との排他的論理和を出力する書き込み回路を有し、

前記リニアフィードバックレジスタは、

前記レジスタの値を前記書き込み回路の出力データで書き換えるための書換え手段を有していてもよい。

#### 【0014】

さらに、前記リニアフィードバックレジスタが備える複数のレジスタの数は、前記乱数のビット数よりも多くてもよい。

#### 【0015】

上記のように構成された擬似乱数発生回路では、リニアフィードバックレジスタに、レジスタの所定出力の排他的論理和を出力する第1の排他的論理和回路、及び外部から供給される入力データと第1の排他的論理和回路の出力信号との排他的論理和を複数のレジスタのうちの先頭のレジスタに入力する第2の排他的論理和回路を備えることで、リニアフィードバックレジスタから出力される乱数列がより不規則になり、乱数性が向上する。

#### 【0016】

また、電源投入時に、発振回路が安定発振する前の不安定な第3のクロックを

用いて生成したシフトクロックをリニアフィードバックレジスタに供給することで、リニアフィードバックレジスタの初期値の元になるPre-SEEDの乱数性が高まり、さらに書き込み回路を用いて外部から任意のデータを書き込むことで初期値の乱数性をより高めることができる。

#### 【0017】

また、信号生成回で、第1のクロック、及び第1のクロックを分周したクロックを所定の周期で切り換えたシフトクロックをリニアフィードバックレジスタで用いること、あるいはリニアフィードバックレジスタが備える複数のレジスタの数を生成する乱数のビット数よりも多くすることで、リニアフィードバックレジスタから出力されるデータの乱数性が従来よりも格段に向上する。

#### 【0018】

##### 【発明の実施の形態】

次に本発明について図面を参照して説明する。

#### 【0019】

図1に示すように、本発明の擬似乱数発生回路は、LFSR1と、LFSR1を動作させるためのクロックであるシフトクロック (LSFR clock) 及び入力データ (data in) を生成する信号生成回路2と、LFSR1で生成された擬似乱数の読み出しを制御するアクセスコントローラ3と、LFSR1の各レジスタに外部から入力されるデータを書き込むための書き込み回路4とを有する構成である。また、図2に示すように、本実施形態の擬似乱数発生回路には、電源投入後のリセット期間においてLFSR1の初期値 (SEED) の元になるPre-SEEDを生成するためのPre-SEED回路5が接続される。

#### 【0020】

本実施形態では、擬似乱数発生回路の構成を、後述する動作の説明を容易にするために、通常動作時の構成を図1に示し、電源投入後のリセット期間の構成を図2に示している。実際の擬似乱数発生回路はこれらの構成要素を全て備えたものであり、LFSR1への入力通常動作時あるいはリセット期間に応じて切り換えられる。なお、回路が動作する上で影響が無いなら、これらの入力は切り換える必要は無く、信号生成回路2の出力信号及びPre-SEED回路5の出力信号が常

時入力されていてもよい。

#### 【0021】

図1に示す信号生成回路2に供給される第1のクロックCLK1は、例えばリングオシレータ等によって生成された一定周期のクロックであり、第2のクロックCLK2は、水晶発振器等を備えた不図示の発振回路あるいは外部から供給されるクロックを第1のクロックCLK1にフリップフロップ等を用いて同期させたクロックである。

#### 【0022】

また、図2に示すPre-SEED回路5に供給される第3のクロックCLK3は、第1のクロックCLK1と同様にリングオシレータ等の発振回路6によって生成された一定周期のクロックであり、第4のクロックCLK4は、水晶発振器等を備えた不図示の発振回路あるいは外部から供給される第1のクロックCLK1と非同期のクロックである。

#### 【0023】

第3のクロックCLK3は、後述するようにPre-SEEDの乱数性を高めるため、リングオシレータ等の発振回路6の出力クロックをそのまま使用するのが好ましい。第1のクロックCLK1は、このような制限はなく、発信回路6の出力クロックをそのまま使用してもよく、例えば出力クロックを停止させるための不図示の制御回路を通過したクロックを使用してもよい。

#### 【0024】

図1に示すように、本実施形態のLSFR1は、直列に接続された複数のレジスタと、レジスタの所定出力の排他的論理和を出力する第1のXOR回路(XOR1)と、信号生成回路2から供給される入力データと第1のXOR回路の出力信号との排他的論理和を先頭のレジスタに入力する第2のXOR回路(XOR2)とを有する構成である。このように、第2のXOR回路によって先頭のレジスタに帰還させる信号に信号生成回路2から供給される入力データでモジュレーションをかけることで、図3に示すようにLFSR1から出力されるデータ列がより不規則になり、乱数性が向上する。

#### 【0025】

また、本実施形態の擬似乱数発生回路では、生成する乱数のビット数よりも度数が多い LFSR1 を使用する。例えば 16 ビットの擬似乱数を生成する場合、本実施形態では 26 ビットの LFSR1 を使用する。これは、上述したように 16 ビットの LFSR1 を使用して乱数を生成するよりも乱数性が高くなるためである。

#### 【0026】

また、本実施形態では、LFSR1 から出力されるデータの乱数性をより高くするため、信号生成回路 2 によって生成されるシフトクロックの周波数を所定期毎に切り換える。具体的には、第 1 のクロック CLK1 をシフトクロックとして用い、周波数を変えないクロック (Full) と周波数を  $1/2$  に分周したクロック (Half) とを自動的に切り換える。なお、分周したクロックは、第 1 のクロック CLK1 の  $1/2$  の周波数である必要はなく、 $1/4$ 、 $1/8$ 、 $1/16$  等、いくつであってよい。

#### 【0027】

通常動作時、LFSR1 はシフトクロックが入力される度に乱数を生成するが、乱数はクロック毎に読み出しができないようにする。すなわち、アクセスコントローラ 3 の制御により LFSR1 で生成される乱数列のなかから、所定の周期毎に乱数を読み出すようにする。

#### 【0028】

書き込み回路 4 は、LFSR1 の初期値 (SEED) の乱数性をより高めるために、ユーザが外部から LFSR1 の各レジスタに任意のデータを書き込むためのものであり、LFSR1 の出力データとユーザが書き込むデータである書き込み信号との排他的論理和を出力する複数の XOR 回路を備えている。書き込み回路 4 は、例えば生成する初期値のビット数分だけ XOR 回路を備え、各 XOR 回路の出力信号は、不図示のセレクタ等 (書換え手段) を介して LFSR1 の所定のレジスタに入力される。

#### 【0029】

図 2 に示すように、Pre-SEED 回路 5 は、第 3 のクロック CLK3 と第 4 のクロック CLK4 との排他的論理和を出力し、LFSR1 にシフトクロックとして供給する X

OR回路を備えた構成である。リセット期間時、第4のクロックCLK4はLFSR1に入力データとして供給される。

#### 【0030】

次に、本発明の擬似乱数発生回路の動作について図面を参照して説明する。

#### 【0031】

上述したように、本実施形態の擬似乱数生成回路は、動作を電源投入後のリセット期間と通常動作時との2つに分けることができる。まず、リセット期間の動作について図2を参照して説明する。

#### 【0032】

上述したように、リセット期間においてLFSR1に供給される第3のクロックCLK3にはリングオシレータ等の発振回路6の出力クロックがそのまま使用される。リセット期間は電源投入直後の期間であるため、リングオシレータは発振が安定せず第3のクロックCLK3の周波数も不安定となる。本実施形態では、この不安定なクロックをLFSR1のシフトクロックとして使用することでLFSR1で生成されるPre-SEEDの乱数性を高めている。

#### 【0033】

また、本実施形態では、第3のクロックCLK3と、第3のクロックCLK3に対して非同期的な第4のクロックCLK4との排他的論理和出力をLFSR1にシフトクロックとして供給するため、乱数性がより高いPre-SEEDを得ることができる。

#### 【0034】

次に、本実施形態の擬似乱数生成回路の通常動作について図1を参照しつつ図4～図10を用いて説明する。

#### 【0035】

図4は図1に示した信号生成回路が備える入力データを生成する回路の一構成例を示す回路図であり、図5は図4に示した回路の動作を示すタイミングチャートである。図6は図1に示した信号生成回路が備えるシフトクロックを生成するための回路の一構成例を示す回路図であり、図7は図6に示した回路の動作を示すタイミングチャートである。図8は図1に示したアクセスコントローラの一構成例を示す回路図であり、図9は図8に示した回路の動作を示すタイミングチャ

ートである。また、図10は図1に示したアクセスコントローラの動作を示す模式図である。

#### 【0036】

リセット期間が終了後、本実施形態の擬似乱数発生回路では、まず、リセット期間中に生成されたPre-SEEDを基にLFSR1の初期値であるSEEDを生成する。そして、信号生成回路2から出力されるシフトクロックのタイミングで該SEEDから始まる擬似乱数列を順次生成する。なお、本実施形態では、上述したようにユーザが外部からLFSR1の各レジスタに任意のデータを書き込むための書き込み回路4を備え、ユーザが入力したデータ（書き込み信号）とLFSR1で生成した初期値との排他的論理和出力をLFSR1の各レジスタに書き込むことが可能である。このような機能を利用すれば、さらに乱数性の高いSEEDを得ることができる。SEEDが生成されると、LFSR1は該SEEDから始まる乱数列を順次生成する。このとき、信号生成回路2では図4及び図6に示す回路を用いてシフトクロックの周波数を所定周期毎に切り換える。

#### 【0037】

図4は、LFSR1の入力データ（data in）と、シフトクロックの周波数の変更タイミングを制御するためのクロックスピード制御信号（speed cont sig.）を生成する回路例であり、第2のクロックCLK2を第1のクロックCLK1でフリップフロップ（F/F）を用いてラッチした後（図5のA）、その立ち上がりエッジ及び立下りエッジを論理ゲートにより検出する（図5のB、C）。そして、第2のクロックCLK2の立ち上がりで“1”から“0”または“0”から“1”に反転する入力データ（図5のdata in）を生成し、第2のクロックCLK2の立ち下がりで“1”から“0”または“0”から“1”に反転するクロックスピード制御信号（図5のspeed cont sig.）をそれぞれ生成する。

#### 【0038】

さらに、クロックスピード制御信号（speed cont sig.）は、図6に示す回路に入力され、シフトクロックの周波数を制御するためのクロックイネーブル信号（clk enable）が生成される。クロックイネーブル信号（clk enable）は、4値セクタ（MUX）の出力をラッチすることで生成され、4値セクタの切り換え

信号としてクロックスピード制御信号 (speed cont sig.) が使用される。すなわち、図7に示すように、クロックスピード制御信号 (speed cont sig.) が “0” のとき、4 値セクタ (MUX) の出力をラッチするラッチ回路 (F/F) は第1のクロックCLK1の立ち上がりタイミングで入力端子Dから入力される前値の反転値を出力し、第1のクロックCLK1を2分周した信号をクロックイネーブル信号 (clk enable) として出力する。

#### 【0039】

一方、クロックスピード制御信号 (speed cont sig.) が “1” のとき、4 値セクタ (MUX) の出力をラッチするラッチ回路 (F/F) は、入力端子Dから入力される値が “1” で固定されているため、クロックイネーブル信号 (clk enable) として固定値 “1” を出力する。

#### 【0040】

シフトクロックは、クロックイネーブル信号と第1のクロックCLK1とを入力とするゲート回路を通過させることで生成する。その結果、クロックイネーブル信号が “1” のときは第1のクロックCLK1がそのまま出力され、クロックイネーブル信号が “0” のときは第1のクロックCLK1の  $1/2$  の周波数のシフトクロックが出力される。

#### 【0041】

なお、図4及び図6に示す回路は、擬似乱数発生回路の試験時にテスト切換信号を用いて試験用の入力信号に切り換えることが可能であり、第2のクロックCLK2、入力データ (data in) 、及びクロックスピード制御信号 (speed cont sig.) は、それぞれセクタ (MUX) によって外部から供給されるテストクロック、テストデータ、テスト制御信号に切り換えることができる。また、テスト切換信号が有効 (“1”) のとき、図6に示すtst init value信号の値が有効になる。

#### 【0042】

アクセスコントローラ3は、LFSR1で生成された乱数を所定の周期毎に読み出すための読み出しタイミングを生成する回路であり、例えば図8に示すように、3ビットのLFSRを用いたカウンタ回路を備えた構成である。

#### 【0043】

本実施形態の擬似乱数発生回路から乱数を読み出す場合、外部から読み出し用制御信号 (req sampling) が入力される。アクセスコントローラ 3 は、読み出し用制御信号を受け取ると、3 ビットの L F S R の動作を開始させ、第 1 のクロック CLK1 を所定数だけカウントした後 (図 8 の構成では 6)、乱数リード許可信号 (req sampling) を生成する。この乱数リード許可信号 (req sampling) が出力されると、例えば不図示のレジスタにその時点で格納されている、L F S R 1 で生成された乱数が出力される。カウンタ回路のカウント数はいくつであってもよく、乱数の読み出し周期はカウンタ回路の構成を変えることで変更可能である。例えば、図 10 は 16 クロック毎に乱数を読み出される様子を模式的に示している。

#### 【0044】

以上説明したように、本発明の構成によれば、L F S R 1 に、レジスタの所定出力の排他的論理和を出力する第 1 の X O R 回路、及び信号生成回路 2 から供給される入力データと第 1 の X O R 回路の出力信号との排他的論理和を先頭のレジスタに入力する第 2 の X O R 回路を備え、第 2 の X O R 回路によって先頭のレジスタに帰還させる信号に外部から供給される入力データでモジュレーションをかけることで、L F S R 1 から出力される乱数列がより不規則になり、乱数性が向上する。

#### 【0045】

また、電源投入時に、発振回路 6 が安定発振する前の不安定な第 3 のクロック CLK3 を用いて生成したシフトクロックを L F S R 1 に供給し、L F S R 1 の初期値 (SEED) の元になる Pre-SEED を生成することで該 Pre-SEED 及び SEED の乱数性が高まる。さらに書き込み回路 4 を用いて外部から任意のデータを書き込むことで SEED の乱数性をより高めることができる。

#### 【0046】

また、信号生成回 2 で、第 1 のクロック CLK1、及び第 1 のクロック CLK1 を分周したクロックを所定の周期で切り換えることで生成したシフトクロックを L F S R 1 で用いること、あるいは L F S R 1 が備える複数のレジスタの数を生成する乱数のビット数よりも多くすることで、L F S R 1 から出力されるデータの乱数



性が従来よりも格段に向上する。

**【0047】**

したがって、高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を得ることができる。

**【0048】**

**【発明の効果】**

本発明は以上説明したように構成されているので、以下に記載する効果を奏する。

**【0049】**

リニアフィードバックレジスタに、レジスタの所定出力の排他的論理和を出力する第1の排他的論理和回路、及び外部から供給される入力データと第1の排他的論理和回路の出力信号との排他的論理和を複数のレジスタのうちの先頭のレジスタに入力する第2の排他的論理和回路を備えることで、リニアフィードバックレジスタから出力される乱数列がより不規則になり、乱数性が向上する。

**【0050】**

また、電源投入時に、発振回路が安定発振する前の不安定な第3のクロックを用いて生成したシフトクロックをリニアフィードバックレジスタに供給することで、リニアフィードバックレジスタの初期値の元になるPre-SEEDの乱数性が高まり、さらに書き込み回路を用いて外部から任意のデータを書き込むことで初期値の乱数性をより高めることができる。

**【0051】**

また、信号生成回で、第1のクロック、及び第1のクロックを分周したクロックを所定の周期で切り換えたシフトクロックをリニアフィードバックレジスタで用いること、あるいはリニアフィードバックレジスタが備える複数のレジスタの数を生成する乱数のビット数よりも多くすることで、リニアフィードバックレジスタから出力されるデータの乱数性が従来よりも格段に向上する。

**【0052】**

したがって、高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を得ることができる。

**【図面の簡単な説明】****【図 1】**

本発明の擬似乱数発生回路の一構成例を示すブロック図である。

**【図 2】**

図 1 に示した擬似乱数発生回路のリセット期間における構成を示すブロック図である。

**【図 3】**

本発明の擬似乱数発生回路で生成される乱数系列を示す模式図である。

**【図 4】**

図 1 に示した信号生成回路が備える入力データを生成する回路の一構成例を示す回路図である。

**【図 5】**

図 4 に示した回路の動作を示すタイミングチャートである。

**【図 6】**

図 1 に示した信号生成回路が備えるシフトクロックを生成するための回路の一構成例を示す回路図である。

**【図 7】**

図 6 に示した回路の動作を示すタイミングチャートである。

**【図 8】**

図 1 に示したアクセスコントローラの一構成例を示す回路図である。

**【図 9】**

図 8 に示した回路の動作を示すタイミングチャートである。

**【図 1 0】**

図 1 に示したアクセスコントローラの動作を示す模式図である。

**【図 1 1】**

従来の擬似乱数発生回路で生成される乱数系列を示す模式図である。

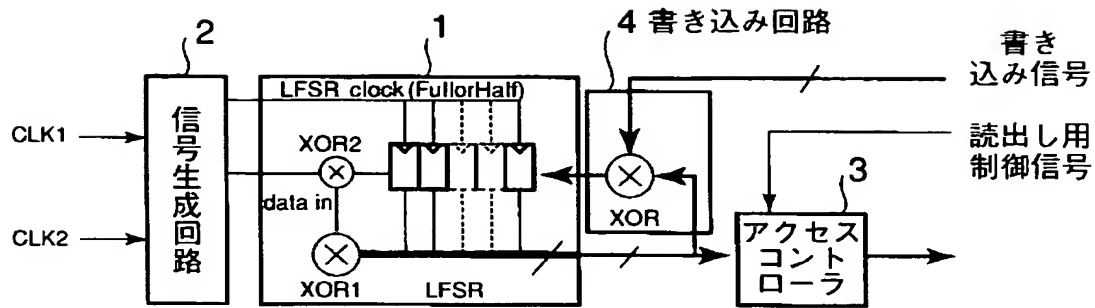
**【符号の説明】**

- 1     L F S R
- 2     信号生成回路

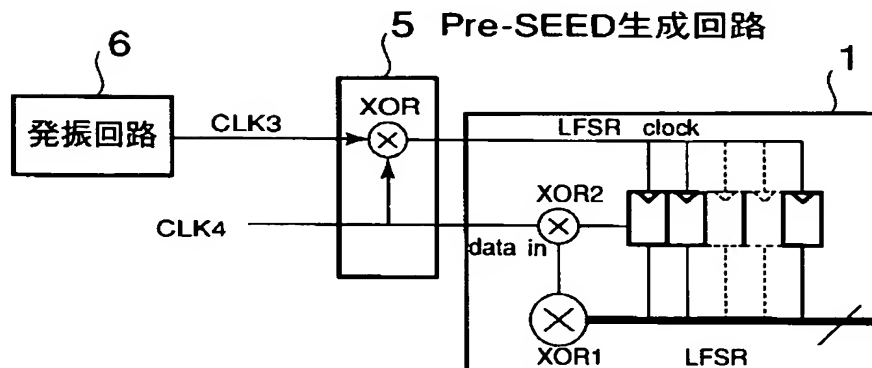
- 3    アクセスコントローラ
- 4    書き込み回路
- 5    Pre-SEED生成回路
- 6    発振回路

【書類名】 図面

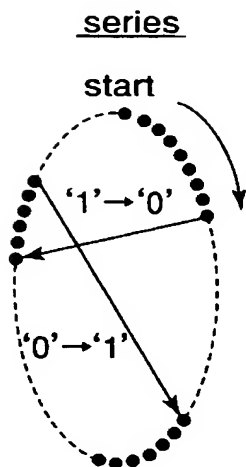
【図1】



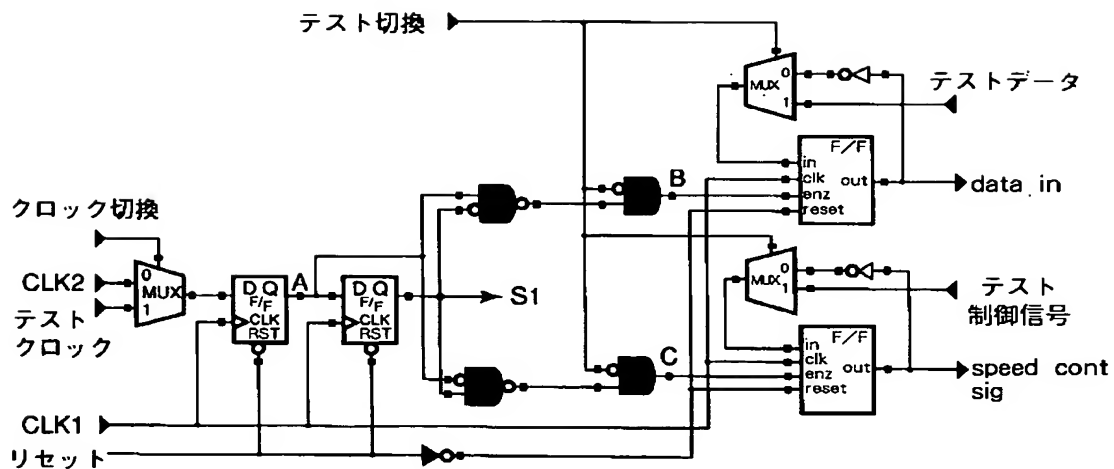
【図2】



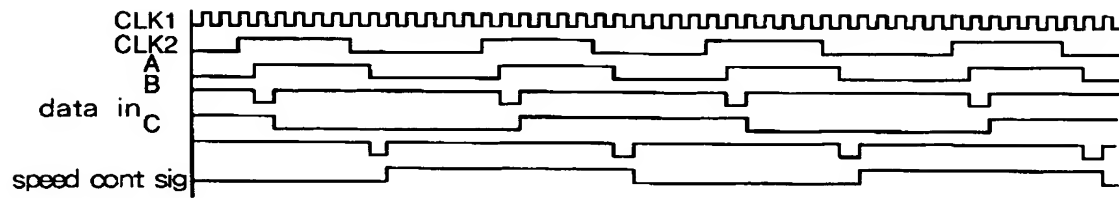
【図 3】



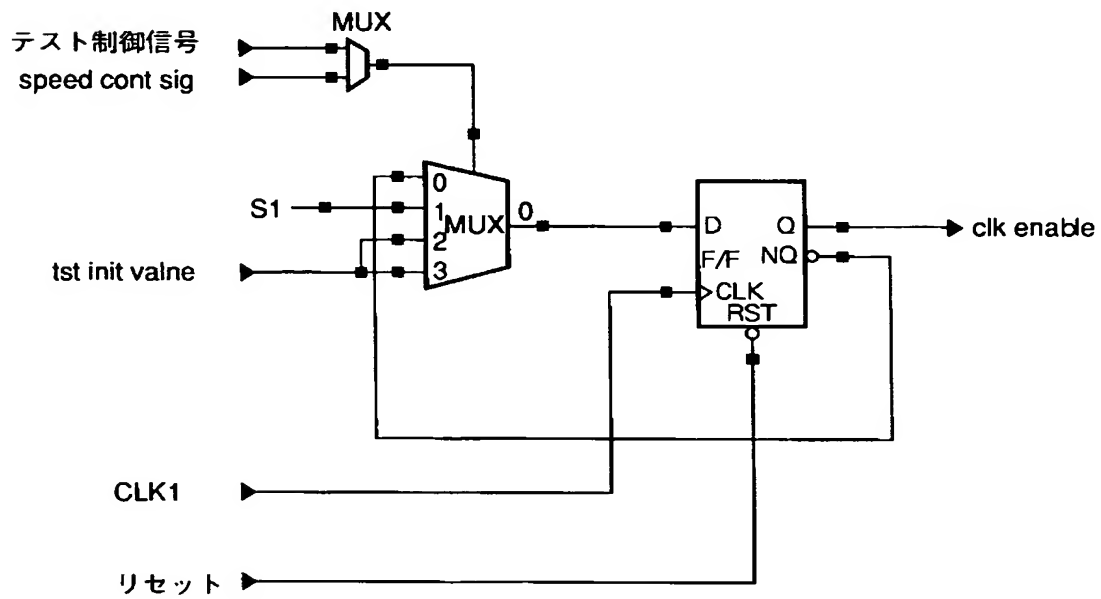
【図 4】



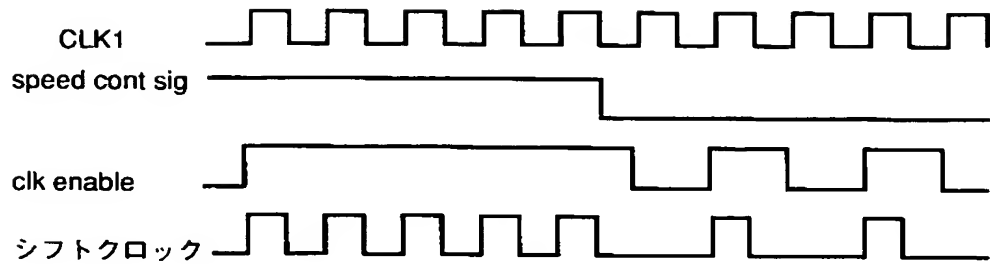
【図 5】



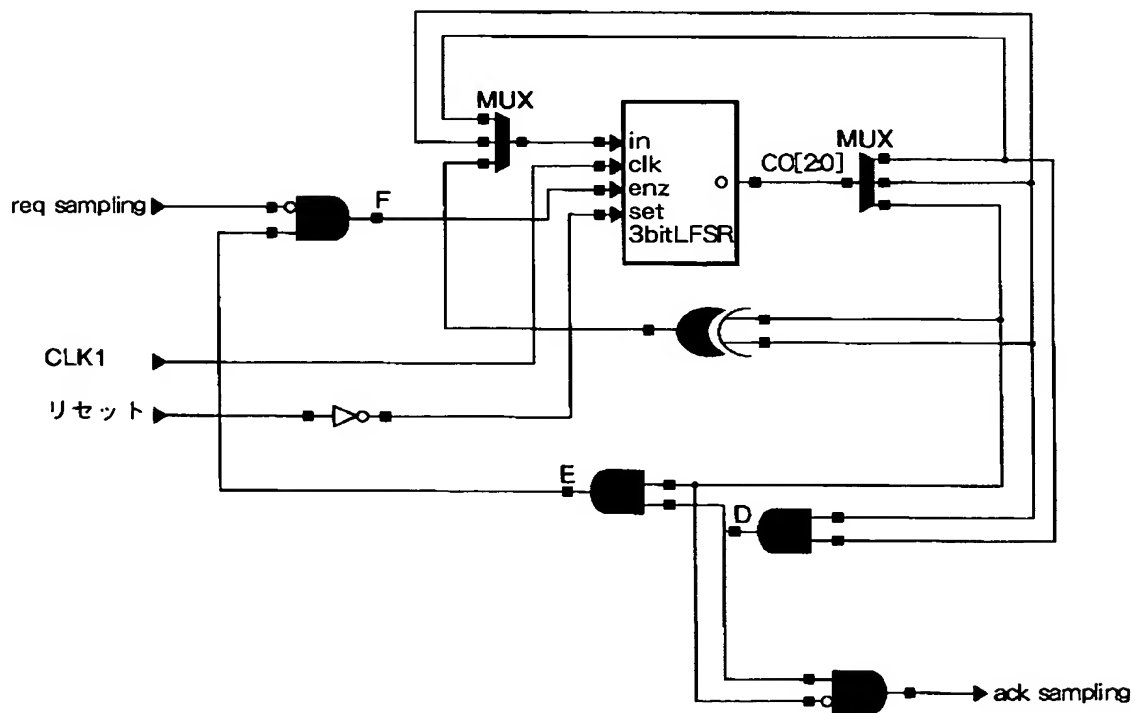
【図 6】



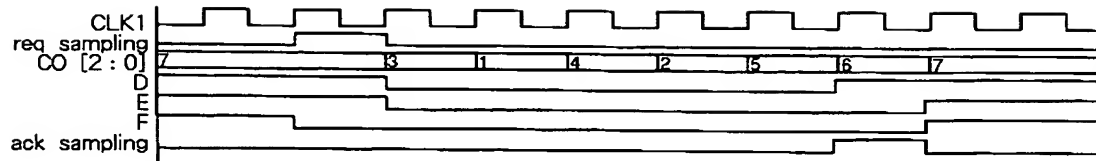
【図 7】



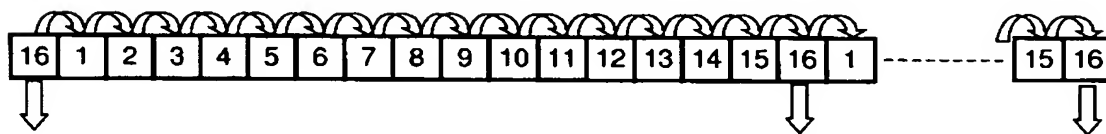
【図 8】



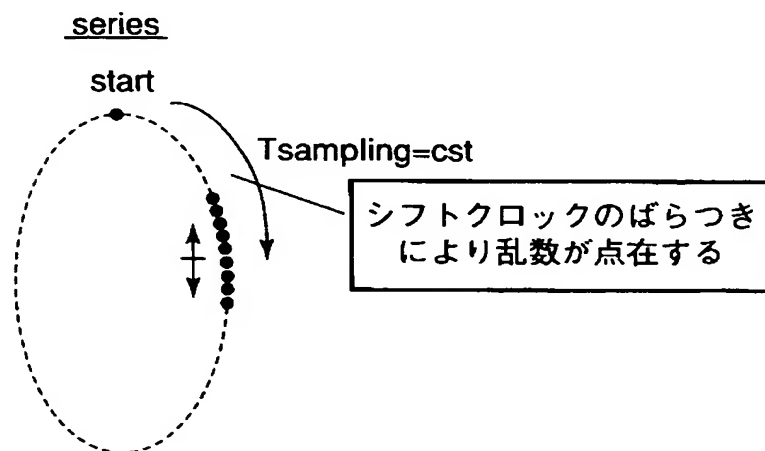
【図 9】



【図 10】



【図 11】





【書類名】 要約書

【要約】

【課題】 高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を提供する。

【解決手段】 直列に接続された複数のレジスタ、該レジスタの所定出力の排他的論理和を出力する第 1 の排他的論理和回路、及び外部から供給される入力データと第 1 の排他的論理和回路の出力信号との排他的論理和を複数のレジスタのうちの先頭のレジスタに入力する第 2 の排他的論理和回路を備えたリニアフィードバックレジスタと、一定周期の第 1 のクロック、及び第 1 のクロックに同期させた第 1 のクロックと異なる周波数の第 2 のクロックを用いて、リニアフィードバックレジスタを動作させるためのクロックであるシフトクロック及び前記入力データを生成する信号生成回路とを有する構成とする。

【選択図】 図 1

特願 2 0 0 3 - 0 9 5 5 9 6

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 2 3 2 0 3 6 ]

1. 変更年月日 2 0 0 1 年 5 月 2 1 日  
[変更理由] 名称変更  
住 所 神奈川県川崎市中原区小杉町 1 丁目 4 0 3 番 5 3  
氏 名 エヌイーシーマイクロシステム株式会社
2. 変更年月日 2 0 0 3 年 7 月 3 0 日  
[変更理由] 名称変更  
住 所 神奈川県川崎市中原区小杉町 1 丁目 4 0 3 番 5 3  
氏 名 N E C マイクロシステム株式会社